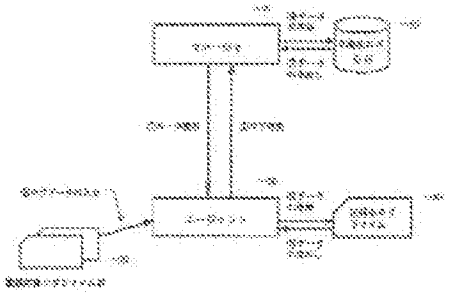
INFORMATION PROCESSOR COLLECTING AND MANAGING LOG DATA

Publication number: JP10293704 (A)
Publication date: 1998-11-04
Inventor(s): FUJINO SHUJI; MORIKAWA TOSHIYOSHI; URANO AKIHIRO; NAKANO HIDENORI; MORITA SHINJI; YAMADA MITSUGI; NIIMURA YOSHITAKA +
Applicant(s): HITACHI LTD +
Classification:
- International: ***G06F11/00; G06F11/34;*** (IPC1-7): G06F11/34
- European: G06F11/34T4; H04L12/24A4; H04L12/24D
Application number: JP19970101210 19970418
Priority number(s): JP19970101210 19970418

Also published as:
JP3778652 (B2)
US6173418 (B1)

Abstract of **JP 10293704 (A)**

PROBLEM TO BE SOLVED: To manage log data based on a common data format and also to manage log data based on the time of a manager in a system in which a manager collects log data from plural agents through a network. SOLUTION: A manager 10 distributes various rules to an agent 20. The agent 20 inputs log data from a monitored object log file group 30 according to the rules, normalizes it, adds the correction time of a log output time and stores it in a normalization log file 40. The agent 20 fetches normalization log data from the file 40 and transfers it to the manager 10 according to a request from the manager 10. The manager 10 stores collected normalization log data in a normalization log database 50 in order of the correction time.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－293704

(43)公開日　平成10年(1998)11月４日

(51)Int.Cl.[6]	識別記号	Ｆｉ	
Ｇ０６Ｆ　11/34		Ｇ０６Ｆ　11/34	Ｂ

審査請求　未請求　請求項の数５　ＯＬ　（全 24 頁）

(21)出願番号　特願平9－101210

(22)出願日　平成９年(1997)４月18日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　藤野　修司
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(72)発明者　森川　寿義
東京都千代田区大手町二丁目６番２号　株式会社日立情報ネットワーク内

(72)発明者　浦野　明裕
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　高橋　明夫

最終頁に続く

(54)【発明の名称】　ログデータの収集と管理をする情報処理装置

(57)【要約】

【課題】　マネージャがネットワークを介して複数のエージェントからログデータを収集するシステムにおいて，共通的なデータ形式に基づいてログデータを管理する。またマネージャの時刻に基づいたログデータを管理する。

【解決手段】　マネージャ１０は，各種ルールをエージェント２０に配布する。エージェント２０は，このルールに従って監視対象ログファイル群３０からログデータを入力し，正規化し，ログ出力時刻の補正時刻を付加して正規化ログファイル４０に格納する。マネージャ１０からの要求に従ってエージェント２０は，正規化ログファイル４０から正規化ログデータを取り出してマネージャ１０へ転送する。マネージャ１０は，収集した正規化ログデータを補正時刻の順に正規化ログデータベース５０に格納する。

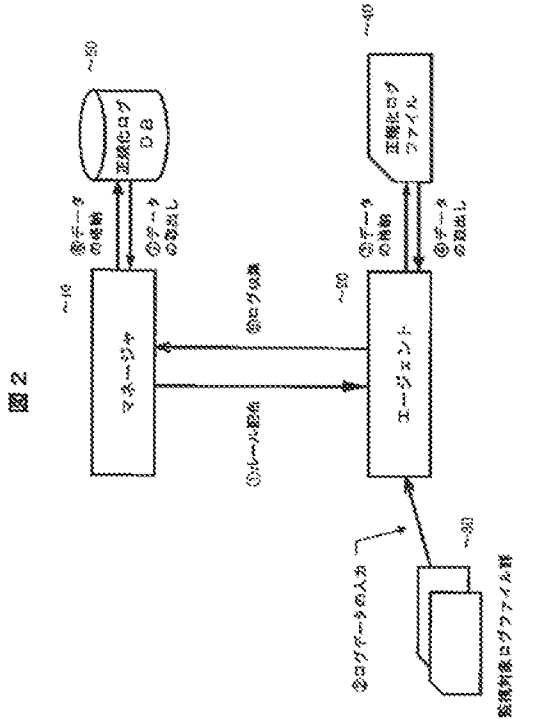


図２

1

【特許請求の範囲】

【請求項１】監視の対象とするログファイル中のログデータからあらかじめ定義されたデータ項目に対応する値を切り出して規定されたデータ項目の値を配列する正規化されたログデータを作成して蓄積する手段と、蓄積された正規化ログデータをネットワークを介してマネージャの機能を実行する情報処理装置へ送信する手段とをエージェントの処理手段として有することを特徴とするログデータの収集をする情報処理装置。

【請求項２】コンピュータ読み取り可能な記憶媒体上に実体化され、ログデータを収集するエージェント機能を有するコンピュータプログラムであって、該プログラムは以下のステップを含む：

（ａ）監視の対象とするログファイル中のログデータからあらかじめ定義されたデータ項目に対応する値を切り出して規定されたデータ項目の値を配列する正規化されたログデータを作成し、（ｂ）蓄積された正規化ログデータをネットワークを介してマネージャの機能を実行するコンピュータへ送信する。

【請求項３】ネットワークを介してエージェントの機能を実行する情報処理装置からあらかじめ定義された共通のデータ形式に従って正規化されたログデータであってマネージャの基準とする時刻に基づいて補正されたログ出力時刻を有する正規化ログデータを受信する手段と、該正規化ログデータを補正時刻の順にデータベースに蓄積する手段とをマネージャの処理手段として有することを特徴とするログデータの収集と管理をする情報処理装置。

【請求項４】該補正時刻とマネージャの現在時刻との差分の時間が所定の保存期間を超過している正規化ログデータを該データベースから抹除する手段をさらに設けることを特徴とする請求項３記載のログデータの収集と管理をする情報処理装置。

【請求項５】コンピュータ読み取り可能な記憶媒体上に実体化され、ログデータの収集と管理をするマネージャ機能を有するコンピュータプログラムであって、該プログラムは以下のステップを含む：

（ａ）ネットワークを介してエージェントの機能を実行するコンピュータからあらかじめ定義された共通のデータ形式に従って正規化されたログデータであってマネージャの基準とする時刻に基づいて補正されたログ出力時刻を有する正規化ログデータを受信し、（ｂ）該正規化ログデータを補正時刻の順にデータベースに蓄積する。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、マネージャがネットワークを介してエージェントからログデータを収集するシステムに係わり、特にマネージャがシステム内に存在するログデータを共通的なログデータ形式に基づいて管理するログデータの収集と管理の方式に関する。

2

【０００２】

【従来の技術】情報処理装置で実行されるオペレーティングシステム（ＯＳ）やアプリケーションプログラムは、各種のログ情報を出力する。出力されたログ情報を収集するいくつかの方式が知られている。例えば特開平５－２５０２２９号公報は、複数のコンピュータからのログデータ収集において、ログデータ中のエラーコードを検出することにより、エラー状態のコンピュータからのログデータを優先的に送信するログデータ収集方式を開示する。また特開平５－２８００８号公報は、情報処理システムが障害ログを収集するとき貯蔵手段に貯えられたログ情報の個数が一定数に達したことを検出し、ログ登録の抑止を行うことにより重要な障害情報の消失を防ぐログ情報収集方式を開示する。また特開平５－１１１０２９号公報は，下位の設備端末からのデータが採取された時刻をデータに付与して上位の制御装置に送ることにより、複数の端末からの各データの時系列的な関係が損なわれることがないようにするデータ収集方式を開示する。

【０００３】

【発明が解決しようとする課題】ネットワークを介して複数のコンピュータが接続され、コンピュータが他のコンピュータと通信しながら処理を進める分散処理システムにおいて，一人のユーザは複数の広範囲に亘るコンピュータやファイルにアクセスし得る。従ってログデータを解析することによってコンピュータやファイルへの不正なアクセスを検出するためには、個々のコンピュータが出力するログデータを中央のコンピュータに集約し、データベースに蓄積する必要がある。しかしながら各種のシステムプログラムやアプリケーションプログラムが出力するログデータは、各々そのデータ形式が異なっているので、単に個々のコンピュータプログラムが出力するログデータを収集して集約するだけではログデータの解析が困難である。また個々のコンピュータが保有する時刻がすべてのコンピュータに亘って一致しているとは限らないので、一般に個々のログデータに付与されている時刻にはずれが生じており、集約されたログデータを正しい時刻の順序に従って配列することが困難である。

【０００４】本発明は、上記の事情に鑑みてなされたものであり，その目的とするところは，共通的なデータ形式に正規化されたログデータを管理することにある。

【０００５】本発明の他の目的は、各サイトのコンピュータからログデータを収集する中央のコンピュータの時刻を基準とするログデータを管理することにある。

【０００６】

【課題を解決するための手段】上記目的を達成するため，本発明は，監視の対象とするログファイル中のログデータからあらかじめ定義されたデータ項目に対応する値を切り出して規定されたデータ項目の値を配列する正規化されたログデータを作成して蓄積する手段と、蓄積

された正規化ログデータをネットワークを介してマネージャの機能を実行するコンピュータへ送信する手段とをエージェントの処理手段として有するログデータの収集をするコンピュータを特徴とする。

【０００７】また本発明は，ネットワークを介してエージェントの機能を実行するコンピュータからあらかじめ定義された共通のデータ形式に従って正規化されたログデータであってマネージャの基準とする時刻に基づいて補正されたログ出力時刻を有する正規化ログデータを受信する手段と、該正規化ログデータを補正時刻の順にデータベースに蓄積する手段とをマネージャの処理手段として有するログデータの収集と管理をするコンピュータを特徴とする。

【０００８】

【発明の実施の形態】以下、本発明の一実施形態について図面に基づいて詳細に説明する。

【０００９】図１は，本発明を適用する通信ネットワークの一例を示すシステム構成図である。ネットワークは複数のＬＡＮ１，３，４及びＷＡＮ（ワイド・エリア・ネットワーク）２に結合されるものである。マネージャ１０は、計算機の主記憶装置に格納され、ＯＳの下で走行するアプリケーションプログラム（ＡＰ）である。エージェント２０は、サーバ等の計算機の主記憶装置に格納され、ＯＳの下で走行するＡＰである。マネージャ１０は、ＬＡＮ１，３，４又はＷＡＮ２を介してエージェント２０－１，２０－２，２０－３，２０－４と通信することが可能である。図に示すように、エージェント２０を実行する計算機はエージェント２０と並行して他のＡＰを実行することが可能である。マネージャ１０を実行する計算機もマネージャ１０と並行して他のＡＰを実行することが可能であるが、充分なＣＰＵ性能と資源を確保するためには、専用の計算機を割り当てるのが望ましい。６０はこのネットワークシステムを管理するネットワーク管理システムであり、ネットワーク管理プログラム及び図示しないネットワーク監視端末から構成される。ネットワーク管理システム６０は、ネットワーク資源についての情報をマネージャ１０に提供する。

【００１０】図２は、マネージャとエージェントが行う処理動作の概略を示す図である。マネージャ１０は、定義された各種ルールをエージェント２０へ配布する(①)。エージェント２０は、受信したルールを登録し、そのルールに従い監視対象ログファイル群３０からログデータを入力し(②)、ログデータを正規化した後、正規化ログファイル４０に格納する(③)。このとき正規化ログデータ中のログ出力時刻をマネージャ１０の時刻を基準とする補正時刻によって補正する。エージェント２０

は、マネージャ１０からログ収集要求があったとき正規化ログファイル４０から正規化されたログデータを取り出し(④)、マネージャ１０へ転送する(⑤)。マネージャ１０は、収集した正規化ログデータを補正時刻の順に正規化ログデータベース５０に格納する(⑥)。またマネージャ１０は、必要に応じて正規化ログデータベース５０から任意の正規化ログデータを抽出し、その解析を行う。

【００１１】図３は、マネージャ１０の構成を示す機能ブロック図である。ルール１１０は定義された各種ルールであり、記憶装置に格納される。正規化ログデータベース５０は、収集された正規化ログデータを格納するデータベースであり、記憶装置に格納される。ネットワーク管理システム６０は、ネットワークを介してマネージャ１０を格納する計算機と接続される他の計算機およびネットワークを監視する端末装置から構成されるシステムであり、マネージャ１０と同じ計算機で走行するネットワーク管理プログラムは、ネットワークの構成要素である各通信回線、ルータ、中継機、各種計算機、計算機のプログラム等の動作状態（接続中／接続断，動作中／停止状態など）、各ネットワーク構成要素の所在場所などを管理する。以下マネージャ１０を構成する各機能モジュールの機能の概略について述べる。

【００１２】（１）ルール定義１００

運用者が各種ルールを定義するためのプログラムツールであり、図示しない入力装置及び表示装置を介してユーザが容易にルールを設定できるようなＧＵＩ（グラフィカル・ユーザ・インタフェース）を提供する。

【００１３】（２）スケジューラ１０１

ルール配布及びログ収集を実行する契機をそれぞれルール配布１０６及びログ収集１０７に知らせるプログラムである。契機の例として、例えば毎日午後５時、毎週土曜日の午後３時１５分などのように実行開始を指示する。

【００１４】（３）プロセス管理１０２

マネージャ１０の１００～１０９を付す各機能モジュールの起動／停止を制御するプログラムである。

【００１５】（４）ログ解析１０３

データベース管理１０９を介して正規化ログデータベース５０から正規化ログデータ群を抽出し、所定の解析を行うプログラムである。以下ログ事象がログインである場合のログデータ解析の例を表１に示す。ログ事象及び正規化項目については後述する。

【００１６】

【表１】

ログデータ解析の例（表１）

ログ解析項目	使用する正規化項目
規定のログイン地域でない所からログインし成功した	ユーザ名 接続元ホスト名 接続元ＩＰアドレス
規定の時間外にログインして失敗した	ユーザ名 開始時刻
同一ユーザが別々の地域から同時にログインしている	ユーザ名 接続元ホスト名
一定期間に規定回数以上のログイン回数がありログインに失敗した	ログ事象 ログ事象結果 ユーザ名 補正時刻
規定回数以上，ユーザ名とパスワードの組み合わせを失敗したユーザ変更を行った	ログ事象 ログ事象結果 ユーザ名 変更後のユーザ名 補正時刻

【００１７】（５）構成管理１０４
対象とするエージェント２０の一覧を管理するプログラムである。またネットワーク管理システム６０に問い合わせを行ってエージェント２０が動作する計算機の動作有無やｐｉｎｇの応答時間等の情報を取得してルール配布１０６又はログ収集１０７に渡す。
【００１８】（６）ルール管理１０５
ルール定義１００から定義された各種ルールを受け取ってルール１１０に格納する。またルール１１０からルールを読み出してルール配布１０６に渡す。
【００１９】（７）ルール配布１０６
スケジューラ１０１の指示に従い，ルール管理１０５から各種ルールを取得してエージェント２０へ配布するプログラムである。
【００２０】（８）ログ収集１０７
スケジューラ１０１の指示に従い，エージェント２０から正規化ログファイルを収集するプログラムである。
【００２１】（９）データ通信１０８
ルール配布１０６及びログ収集１０７がエージェント２０と通信するときに通信制御を行うプログラムである。
【００２２】（１０）データベース管理１０９
ログ収集１０７がエージェント２０から収集した正規化ログデータ群（正規化ログファイル）を正規化ログデータベース５０に格納し，ログ解析１０３からの要求によって正規化ログデータを検索し抽出する。また所定の保存期間を過ぎた正規化ログデータを正規化ログデータベース５０から削除し，未使用の記憶領域を生み出す。
【００２３】図４は，エージェント２０の構成を示す機能ブロック図である。ルール２０５は配布を受けた各種ルールであり，記憶装置に格納される。監視対象ログファイル群３０は，監視対象とするログファイルであり，記憶装置に格納される。正規化ログファイル４０は，正規化ログデータを格納するファイルであり，記憶装置に格納される。以下エージェント２０を構成する各機能モジュールの機能の概略について述べる。
【００２４】（１）データ通信２００
データ通信２００は，ルール管理２０３及びログファイル管理２０４がマネージャ１０と通信するときに通信制御を行うプログラムである。
【００２５】（２）プロセス管理２０１
エージェント２０の２００～２０４を付す各機能モジュールの起動／停止を制御するプログラムである。
【００２６】（３）ログ入力２０２
ルール管理２０３からログファイル監視ルールやフォーマットルール等を取得し，監視対象ログファイル群３０から入力したログデータを正規化した後，正規化ログデータをログファイル管理２０４へ渡すプログラムである。
【００２７】（４）ルール管理２０３
マネージャ１０から配布された各種ルールをルール２０５として記憶装置に格納し，ログ入力２０２又はログファイル管理２０４の要求に応じてルールを提供するプログラムである。
【００２８】（５）ログファイル管理２０４
ルール管理２０３からフィルタリングルールを取得し，ログ入力２０２から受け取った正規化ログデータをフィルタリングし，補正時刻を付加して正規化ログファイル４０に格納する。マネージャ１０のログ収集１０７から正規化ログファイル４０の収集要求を受信したとき，正規化ログファイル４０をマネージャ１０へ転送する。
【００２９】図５～図１４は，正規化ログデータの構造の一例を示す図である。

7

【００３０】図５は、正規化ログファイル４０に格納される正規化ログデータ３００の概略構成を示す図である。正規化ログデータ３００は、共通情報クラス３０１と必要に応じて追加されるユーザ情報クラス３０２、サービス情報クラス３０３、アドレス情報クラス３０４，ファイル情報クラス３０５，トラフィク情報クラス３０６、個別情報クラス３０７等から構成される。共通情報クラス３０１は、すべての正規化ログデータ３００に必須の情報クラスであり、残りの情報クラスは出力されたログデータに応じて選択されるものである。

【００３１】図６は、共通情報クラス３０１のデータ構成を示す図である。正規化バージョン３１０は、正規化のバージョンを示す番号である。ログ種別はログ事象３１１，ログ事象結果３１２、ログ出力プログラム３１３、データ格納クラス３１４及びログファイル名３１５を含む。ログ出力プログラム３１３はログを出力したＯＳ又はＡＰの名称であり、ログファイル名３１５はログ出力プログラム３１３が出力したログファイルの名称である。ログ事象３１１、ログ事象結果３１２及びデータ格納クラス３１４については後述する。マネージャは、マネージャを搭載する計算機のホスト名３１６とホストＩＰアドレス３１７を格納する。エージェントは、ログを入力したエージェントを搭載する計算機のホスト名３１８とホストＩＰアドレス３１９を格納する。監視対象は、監視対象とするサーバ等の計算機のホスト名３２０とホストＩＰアドレス３２１を格納する。時刻はログ出力時刻３２２と補正時刻３２３から成る。ログ出力時刻３２２はログを出力した計算機の局所的な時刻であり、補正時刻３２３はマネージャ１０を搭載する計算機の時刻に基づいて補正した時刻である。フィルタリングルール名３２４は、ログデータを正規化するときに適用したフィルタリングルールの名称である。

【００３２】図７は、ユーザ情報クラス３０２のデータ構成を示す図である。ユーザ情報クラス３０２は，ログインしたユーザに関する情報を記録するものであり、ユーザ名３３０、ユーザＩＤ（ＵＩＤ）３３１、ユーザ変更した後のユーザ名３３２、変更後のＵＩＤ３３３、ユーザのセキュリティレベル３３４，計算機やファイルへのアクセス権３３５、アクセスした結果３３６及びユーザが操作した端末装置の名称（端末名３３７）を格納する。

【００３３】図８は、サービス情報クラス３０３のデータ構成を示す図である。サービス情報クラス３０３は，ユーザに提供したサービスについての情報を記録する。サービスは，サービス名３４０、サービスバージョン３４１、サービス提供のために起動したプロセスの名称（プロセス名３４２）及びプロセスＩＤ３４３を格納する。

【００３４】図９は、アドレス情報クラス３０４のデータ構成を示す図である。アドレス情報クラス３０４は、

8

他計算機とコネクションを行ったときの情報を記録するものであり、接続元及び接続先のホスト名、ＩＰアドレス、ＭＡＣアドレス，ポート番号の他にコネクション状態、コネクションの開始時刻と終了時刻及び他計算機へのアクセス結果を格納する。

【００３５】図１０は、ファイル情報クラス３０５のデータ構成を示す図である。ファイル情報クラス３０５は、ユーザが作成又は変更したファイルについてファイル名、変更前のアクセス情報及び変更後のアクセス情報を記録する。アクセス情報は，ファイルの作成時刻、最終修正時刻、最終アクセス時刻、ファイルのｉ－ｎｏｄｅ番号、アクセス許可の有無，ＵＩＤ、グループＩＤ（ＧＩＤ）及び最終的なファイルのサイズを格納する。

【００３６】図１１は、トラフィク情報クラス３０６のデータ構成を示す図である。トラフィク情報クラス３０６は、メール管理プログラム，ファイル転送プログラム，等が出力するログ情報であり、ネットワークを介するデータやメッセージの受信バイト数，送信バイト数及びデータの転送時間（処理時間）を記録する。

【００３７】図１２は，個別情報クラス３０７のデータ構成を示す図である。個別情報クラス３０７は、オプションであり、プログラムが出力するメッセージテキストの原文そのままの情報である。

【００３８】図１３は、データ格納クラス３１４のデータ構造を示す図である。”Ｔ１”はデータ格納クラス３１４を識別するためのタグであり、”Ｌ１”は存在する情報クラスを指定する領域Ｖ１の長さを示す。”Ｖ１”は、各正規化ログデータ３００に含まれる情報クラスを指定する領域であり、情報クラスの指定の開始を示すタグ、情報クラス識別子の長さ及び情報クラス識別子を順番に指定する。情報クラス識別子の長さは可変長である。各情報クラスを識別する番号をｘとすると、Ｔｘ（ｘ≧２）は情報クラスの開始を示すタグであり、Ｌｘ（ｘ≧２）はそのＶｘの部分の長さであり、Ｖｘ（ｘ≧２）は情報クラス識別子である。マネージャ１０は、このデータ格納クラス３１４により各正規化ログデータが有する情報クラスを認識する。

【００３９】図１４は、正規化項目のうちコード化が可能なもののコード化テーブル６００の一例を示す図である。正規化項目のログ事象３１１が“ｌｏｇｉｎ”の場合はコード”１”に，ユーザ変更“ｓｕ”の場合はコード“２”というようにコード化される。コネクト（ｃｏｎｎｅｃｔ）は、計算機間でファイル転送やプログラム間通信を行う際のコネクションに関するログ事象を示す。ファイルは内容変更されたファイルに関するログ事象、ジョブはジョブの起動／停止／終了状態に関するログ事象である。メールはメール使用に関するログ事象を示す。ログ事象結果３１２はログ事象の結果であり、成功か失敗かを区分する。ユーザ情報クラス３０２のアクセス権３３５についてはあり又はなしを区分する。ユー

ザ情報クラス３０２及びアドレス情報クラス３０４のアクセス結果については，成功か失敗かを区分する。ファイル情報クラス３０５のアクセス許可については，あり又はなしを区分する。

【００４０】図１５～図２０は、ルールのデータ形式を示す図である。

【００４１】図１５は、マネージャルール４５０の一例を示す図である。ＤＢ＿ＭＡＸ４５１は正規化ログデータベース５０が正規化ログデータを保存可能な期間を示す保存期間を定義する。ＲＵＬＥ＿ＭＡＸ４５２はルール配布に使用できる最大の通信路数を定義する。ＬＯＧ＿ＭＡＸ４５３はログ収集に使用できる最大の通信路数を定義する。ルール配布１０６やログ収集１０７は、この多重度数だけ通信路を使用できるが、処理の要求がこの多重度より大きい場合は通信路を順番に使用し、通信路が空くまで待った後、残りの処理を実行する。

【００４２】図１６は、エージェント２０の動作条件ルール４７０の一例を示す図である。ＭＡＮＡＧＥＲ＿ＡＤＤＲＥＳＳ４７１はマネージャのＩＰアドレスを定義し、ＦＩＬＥ＿ＭＡＸＳＩＺＥ４７２は正規化ログファイル４０が使用できる最大の記憶容量を定義する。

【００４３】図１７は、ログファイル監視ルール５００の一例を示す図である。ＴＡＲＧＥＴ＿ＬＯＧは監視対象ログファイル名を定義し、ＦＯＲＭＡＴによりファイルの形式（ＳＥＱ：シーケンシャル形式，ＷＲＡＰ：ラップアラウンド形式）を定義し、ＩＮＴＥＲＶＡＬにより監視間隔の時間（たとえば、１０分間隔）を定義する。ＦＭＴ＿ＮＡＭＥは当該ログファイルを正規化するときに適用するルールを定義する。例により説明すると，

TARGET_LOG:/usr/adm/syslog.log,FORMAT=SEQ,INTERVAL=10m,FMT_NAME=abc;

は、シーケンシャル形式のファイル／ｕｓｒ／ａｄｍ／ｓｙｓｌｏｇ．ｌｏｇを１０分間隔で監視し、フォーマットルールａｂｃにより正規化処理を行うことを示す。ＦＭＴ＿ＮＡＭＥの指定がない場合は、エージェント２０の間で共通のフォーマットルールにより正規化を行う。

【００４４】図１８と図１９は、フォーマットルール５１０及び５１５の一例を示す図である。ログデータがテキスト形式の場合はＦＭＴ＿Ｔを適用し、バイナリ形式の場合はＦＭＴ＿Ｂを適用する。ＲＥＧＴＥＸＴ＝“文字列ｎ”は、ログデータを選択する条件を示し、ログデータ中に文字列ｎが存在すれば、以下に示す規則に従ってログデータを正規化することを示す。＆＆は論理積（ＡＮＤ）を示し、複数の文字列の存在を選択条件とすることができる。｜｜ｔｈｅｎを意味し、以下ログデータの文字列のシーケンスに従って文字列から順に正規化項目を拾って行くことを意味する。正規化項目とは、各情報クラスで定義されるデータ項目のことである。：

は、ログデータの先頭から順番にポインタをずらして正規化項目に対応する値を切り出すための区切り文字である。正規化項目に続いて［］内に指定される文字は，任意のポインタから認識する文字列の長さ、またはその文字列が可変長の場合に認識する最後の文字を指定する。ＳＫＩＰは、ログデータの先頭から順番にポインタをずらしていった場合、正規化項目に関係ない文字列が存在する場合にその文字列を読み飛ばすことを意味し、［］内には読み飛ばす文字数又は認識する最後の文字となる“区切り文字”を指定する。区切り文字を指定した場合は，その区切り文字まで読み飛ばす。以下フォーマットルールの例を挙げる。

（ａ）フォーマットルールＡ

FMT_T:REGTEXT == “SU” && REGTEXT == “+” ｜ログ事象 == “2” ｜ログ事象結果== “0” :SKIP[“ ”]:ログ出力時刻[10]: SKIP[3]:端末名[“ ”]:ユーザ名[“-”]:変更後のユーザ名[“ ”];

（ｂ）フォーマットルールＢ

FMT_T:REGTEXT == “connect” && REGTEXT == “refused” ｜ログ事象 == “3” ｜ログ事象結果 == “1” :ログ出力時刻[15]: 接続先ホスト名[“ “]:プロセス名[“[“]:プロセスＩＤ[“]”]:SKIP[“from ”]:接続元ホスト名[“ “];。

図２１は、ログファイルに格納されているメッセージテキストの原文の例を示す図である。メッセージテキスト５５１及び５６２は、ＯＳが出力するユーザ変更に関するメッセージテキストの例である。メッセージテキスト５５３～５５６は、ＯＳがコネクション時に出力するメッセージテキストである。メッセージテキスト５５６及び５５７は、ＯＳのジョブ管理が出力するメッセージテキストである。

【００４５】メッセージテキスト５５１をフォーマットルールＡによって正規化すると，

・ログ事象３１１＝２（ｓｕ）

・ログ事象結果３１２＝０（成功）

・ログ出力時刻３２２＝１／３０　１１：１８のエポックタイム

・端末名３３７＝ｔｔｙｐ５

・ユーザ名３３０＝ｆｕｊｉｎｏ

・変更後のユーザ名３３２＝ｒｏｏｔ

となる。

【００４６】メッセージテキスト５５４をフォーマットルールＢによって正規化すると、

・ログ事象３１１＝３（ｃｏｎｎｅｃｔ）

・ログ事象結果３１２＝１（失敗）

・ログ出力時刻３２２＝Ｊａｎ　１２　１３：１２：１６のエポックタイム

・接続先ホスト名３６４＝ｈｏｓｔａ

・接続先ＩＰアドレス３５５＝ｈｏｓｔａをＩＰアドレスに変換した値

・プロセス名３４２＝ｆｔｐｄ
・プロセスＩＤ３４３＝１１１１
・接続元ホスト名３５０＝ｈｏｓｔｂ
・接続元ＩＰアドレス３５１＝ｈｏｓｔｂをＩＰアドレスに変換した値
となる。

【００４７】図２０は、フィルタリングルール５２０の一例を示す図であり、ログファイル管理２０４が該当する正規化ログデータだけを格納するためのルールである。ＦＩＬＴはフィルタリングルールであることを示し、正規化項目が指定した文字列やコードであったり、指定した時間帯の正規化ログデータであった場合、そのような条件に適合する正規化ログデータだけを抽出して格納する。＝＝はイコールを、！＝はｎｏｔイコールを、＆＆は論理積ＡＮＤを、｜｜は論理和ＯＲを、－は時間間隔をそれぞれ意味する。

【００４８】図２２は、正規化ログデータベース５０のデータ構造を例示する図である。正規化ログデータベース５０は、正規化ログデータを補正時刻６３０の順に配列して格納する。ある補正時刻６３０から共通情報クラス６３１のログデータにチェインする。また共通情報クラス６３１からこれに続いて存在する情報クラスのログデータに次々とチェインする。情報クラスに対応して示される検索キーは、正規化ログデータを検索するときにキーとして使用される正規化項目を示すものである。また補正時刻６３０から次の補正時刻６３０へチェインが張られている。ユーザは、補正時刻６３０によって、また該当する情報クラスの検索キーを指定することによって正規化ログデータベース５０から目的とする正規化ログデータを効率良く抽出することができる。

【００４９】図２３は、マネージャ１０のルール配布１０６の処理の流れを示すＰＡＤ図である。ルール配布１０６は、初期設定（ステップ７０１）後、プロセス管理１０２から終了要求が来るまでループし（ステップ７０２）、イベントを待つ（ステップ７０３）。イベントには、スケジューラ１０１からのルール配布要求（ステップ７０４）とプロセス管理１０２からの終了要求（ステップ７１２）がある。

【００５０】ルール配布要求（ステップ７０４）を受信した場合は、ルール管理１０５を介して配布するルールと配布先であるエージェント２０の一覧を取得し（ステップ７０５）、構成管理１０４からエージェント２０の動作状態及び応答時間の情報を取得する（ステップ７０６）。取得したエージェント２０のｐｉｎｇ応答時間を応答時間の小さい順番に並べ替える（ステップ７０７）。このとき動作していないエージェント２０については、応答時間を無限大と解釈する。ルールを配布するエージェント２０の数だけループし（ステップ７０８）、エージェント２０が動作している場合（ステップ７０９ＹＥＳ）は応答時間の小さい順番にルールを配布し（ステップ７１０）、エージェント２０が動作していない場合はルール配布失敗のメッセージを出力する（ステップ７１１）。ルール配布に当っては、ＲＵＬＥ＿ＭＡＸ４５２を適用する。配布したルールは、エージェント２０のルール管理２０３に転送される。

【００５１】終了要求を受信した場合は（ステップ７１２）、ループを抜けて終了処理を行う（ステップ７１３）。

【００５２】図２４は、マネージャ１０のログ収集１０７の処理の流れを示すＰＡＤ図である。ログ収集１０７は、初期設定（ステップ８０１）後、プロセス管理１０２から終了要求が来るまでループし（ステップ８０２）、イベントを待つ（ステップ８０３）。イベントには、スケジューラ１０１からのログ収集要求（ステップ８０４）、エージェント２０からの起動通知（ステップ８１１）、及びプロセス管理１０２からの終了要求（ステップ８１６）がある。

【００５３】ログ収集要求を受信した場合は（ステップ８０４）、スケジューラ１０１からログを収集するエージェント２０の一覧を取得し（ステップ８０５），構成管理１０４からこれらのエージェント２０の動作状態及び応答時間の情報を取得するとともに，応答時間の短い順番にエージェント２０をソートする（ステップ８０６）。ログを収集するエージェント２０の数分ループし（ステップ８０７）、エージェントが動作している場合（ステップ８０８ＹＥＳ）はログを収集し（ステップ８０９）、エージェントが動作していない場合（ステップ８０８ＮＯ）はログ収集失敗メッセージを出力する（ステップ８１０）。ログ収集に当っては、ＬＯＧ＿ＭＡＸ４５３を適用する。ログ収集１０７は、エージェント２０のログファイル管理２０４を介して正規化ログファイル４０を収集する。

【００５４】エージェント起動通知を受信した場合は（ステップ８１１），構成管理１０４からエージェント２０とのｐｉｎｇ（ＩＣＭＰエコーリクエスト）の応答時間を取得する（ステップ８１２）。ＩＣＭＰ（Ｉｎｔｅｒｎｅｔ ＣｏｎｔｒｏｌＭｅｓｓａｇｅ Ｐｒｏｔｏｃｏｌ）は、通信ネットワークの管理に関する国際的な標準規格の１つであるアイ・エイ・ビー（ＩＡＢ：Ｉｎｔｅｒｎｅｔ Ａｃｔｉｖｉｔｉｅｓ Ｂｏａｒｄ）の管理標準である。ＩＣＭＰを使用すると、ＩＰノード（例えばコンピュータ）が他のＩＰノードと通信可能であるか否かを確認できる。またｐｉｎｇを使用すると、任意のＩＰノードと通信可能であるか否かの動作状態と応答時間を取得できる。ｐｉｎｇ応答時間を取得できた場合（ステップ８１３ＹＥＳ）は、マネージャ１０の現在時刻にこの応答時間から得られる通信時間を加算した時刻を起動通知を発行したエージェント２０へ通知する（ステップ８１４）。マネージャの時刻をエージェントに伝えるためには、マネージャの時刻にマネージャから

エージェントへの通信時間を加えた時刻を通知すればよい。ｐｉｎｇの応答時間は、マネージャからエージェントとエージェントからマネージャ、つまり行きと返りの通信時間を加えた時間間隔である。そこでｐｉｎｇ応答時間の１／２を通信時間として利用する。すなわちマネージャは、次の計算式によりエージェントの時刻を推定しエージェントへ通知する。

（エージェントの時刻）＝（マネージャの時刻）＋（ｐｉｎｇ応答時間）／２

応答時間を取得できなかった場合（ステップ８１３ＮＯ）、すなわちネットワーク管理システム６０から情報を得られない場合は、単にマネージャ１０の現在時刻をエージェント２０へ通知する（ステップ８１５）。エージェント２０は、マネージャ１０の現在時刻を取得して正規化ログデータの補正時刻３２３に適用する。

【００５５】終了要求を受信した場合は（ステップ８１６）、ループを抜けて終了処理を行う（ステップ８１７）。

【００５６】図２５は、マネージャ１０の構成管理１０４の処理の流れを示すＰＡＤ図である。構成管理１０４は、初期設定（ステップ９０１）後、プロセス管理１０２から終了要求が来るまでループし（ステップ９０２）、イベントを待つ（ステップ９０３）。イベントにはルール配布１０６からのエージェント情報格納要求（ステップ９０４）、ルール配布１０６やログ収集１０７からのエージェント情報取得要求（ステップ９０９）と、プロセス管理１０２からの終了要求（ステップ９１３）がある。

【００５７】エージェント情報格納要求を受信した場合は（ステップ９０４）、ルール配布１０６からルールを配布したエージェント２０の情報を取得する（ステップ９０５）。エージェント２０の情報とは、ルールの配布時刻、配布したルール名などである。ネットワーク管理システム６０と通信可能であるとき（ステップ９０６ＹＥＳ）は、取得したエージェント情報をネットワーク管理システム６０に渡す（ステップ９０７）。ネットワーク管理システム６０は、受信したルール配布の履歴情報をネットワーク管理のために利用可能である。ネットワーク管理システム６０と通信できないとき（ステップ９０６ＮＯ）は、エージェント情報を構成管理１０４が保有するファイルへ格納する（ステップ９０８）。

【００５８】エージェント情報取得要求を受信した場合は（ステップ９０９）、ネットワーク管理システム６０と通信できるとき（ステップ９１０ＹＥＳ）には、ネットワーク管理システム６０からエージェント２０の一覧、動作有無やｐｉｎｇの応答時間等を取得しこれらの情報を要求元に返す（ステップ９１１）。ネットワーク管理システム６０と通信できないとき（ステップ９１０ＮＯ）には、構成管理１０４のファイルからエージェントの一覧についての情報を取得して要求元に返す（ステップ９１２）。

【００５９】終了要求を受信した場合は（ステップ９１３），ループを抜けて終了処理（ステップ９１４）を行う。

【００６０】図２６は、マネージャ１０のデータベース管理１０９の処理の流れを示すＰＡＤ図である。データベース管理１０９は、初期設定（ステップ１００１）し、正規化ログデータベース５０に格納している正規化ログデータの保存期間の確認を要求（ステップ１００２）した後、プロセス管理１０２から終了要求が来るまでループし（ステップ１００３）、イベントを待つ（ステップ１００４）。イベントには、ログ収集１０７からの正規化ログデータ格納通知（ステップ１００５）、ログ解析１０３からの正規化ログデータ抽出要求（ステップ１００８）、データベース管理１０９自身が正規化ログデータの保存期間を確認するための要求（ステップ１０１０）と、プロセス管理１０２からの終了要求（ステップ１０１４）がある。

【００６１】正規化ログデータ格納通知を受けた場合は（ステップ１００５），ログ収集１０７から正規化ログデータを取得し正規化ログデータベース５０に格納する（ステップ１００６）。格納に当っては、図２２のデータ構造に従って正規化ログデータを格納する。正規化ログデータは補正時刻６３０の順に配列されるので、この順に従って正規化ログデータをマージする。また正規化ログデータの保存期間確認を要求する（ステップ１００７）。

【００６２】正規化ログデータ抽出要求を受信した場合は（ステップ１００８）、指定された検索キーにより正規化ログデータベース５０を検索し、その結果抽出したデータを要求元へ応答する（ステップ１００９）。

【００６３】保存期間確認要求（ステップ１０１０）を受信した場合は、正規化ログデータベース５０に格納されている正規化ログデータの一番古い補正時刻６３０と現在時刻の差と、ＤＢ＿ＭＡＸ４５１とを比較し（ステップ１０１１），保存期間より古い正規化ログデータを保存しているときは古い正規化ログデータを削除し（ステップ１０１２）、運用者に知らせるために削除メッセージを出力する（ステップ１０１３）。

【００６４】終了要求を受信した場合は（ステップ１０１４）、ループを抜けて終了処理（ステップ１０１５）を行う。

【００６５】図２７は、エージェント２０のログ入力２０２の処理の流れを示すＰＡＤ図である。ログ入力２０２は、初期設定し（ステップ１１０１），エージェント２０のルール管理２０３からログファイル監視ルール５００とフォーマットルール５１０、５１５等を取得（ステップ１１０２）後、プロセス管理２０１から終了要求が来るまでループし（ステップ１１０３）、イベントを待つ（ステップ１１０４）。イベントには、ログファイ

ル管理２０４からのログ入力中断要求（ステップ１１０５）とログ入力再開要求（ステップ１１０７）、プロセス管理２０１からの終了要求（ステップ１１０９）及び時間監視によるタイマ割り込みがある。

【００６６】ログ入力中断要求を受信した場合は（ステップ１１０５）、ログ入力を中断する（ステップ１１０６）。中断する要因は、正規化ログファイル４０の容量がＦＩＬＥ＿ＭＡＸＳＩＺＥ４７２に達したときである。

【００６７】ログ入力再開要求を受信した場合は（ステップ１１０７）、ログ入力を再開する（ステップ１１０８）。再開する要因は、正規化ログファイルをマネージャ１０へ転送したときである。

【００６８】終了要求を受信した場合は（ステップ１１０９）、ループを抜けて終了処理（ステップ１１１７）を行う。

【００６９】ログファイル監視ルール５００に設定された監視間隔に従ってログファイルの監視時刻になったとき、監視対象ログファイル群３０をオープンし（ステップ１１１１）、このログファイルのファイル管理情報を取得する。ファイル管理情報が前回取得したもの同じか否かを確認する（ステップ１１１２）。同じ場合は（ステップ１１１２ＹＥＳ）、前回オープンしたファイルと同じ内容であるため前回のファイルのオフセットからログデータを入力する（ステップ１１１３）。前回のファイルのオフセットは、当該ファイルについて前回入力済のレコードの次のレコードを指している。異なる場合は（ステップ１１１２ＮＯ）、新しいファイル（前回オープンしたファイルは削除された等）であると解釈し、先頭からログデータを入力する（ステップ１１１４）。その後、入力したログデータを正規化し（ステップ１１１５）、正規化ログデータをログファイル管理２０４へ通知する（ステップ１１１６）。ログデータの正規化は、上記のようにフォーマットルール５１０，５１５等を適用して行う。正規化ログデータをログファイル管理２０４に渡した後、当該ログファイルをクローズし、監視間隔に従って次の監視時刻にタイマを設定する。

【００７０】図２８は、エージェント２０のログファイル管理２０４の処理の流れを示すＰＡＤ図である。ログファイル管理２０４は、初期設定し（ステップ１２０１）、ルール管理２０３から動作条件ルール４７０とフィルタリングルール５２０を取得（ステップ１２０２）した後、プロセス管理２０１から終了要求が来るまでループし（ステップ１２０３）、イベントを待つ（ステップ１２０４）。イベントには、ログ入力２０２からの正規化ログデータ格納通知（ステップ１２０５）、マネージャ１０のログ収集１０７からのログ収集要求（ステップ１２０９）、ログファイル管理２０４自身からの正規化ログファイル容量確認要求（ステップ１２１１）、マネージャ１０のログ収集１０７からのマネージャ時刻の通知（ステップ１２１６）と、プロセス管理２０１からの終了要求（ステップ１２１８）がある。

【００７１】正規化ログデータ格納通知を受信した場合は（ステップ１２０５）、ログ入力２０２から正規化ログデータを取得し（ステップ１２０６），エージェントとマネージャの時間差（ステップ１２１７の処理結果）とログ出力時刻３２２から補正時刻３２３を計算する。ログ入力２０２から取得した正規化ログデータにこの補正時刻３２３を追加して正規化ログファイル４０に格納する（ステップ１２０７）。取得した正規化ログデータにフィルタリングルール５２０を適用して条件に合致する正規化ログデータのみを正規化ログファイル４０に格納する。次に正規化ログファイル容量確認要求を発行する（ステップ１２０８）。

【００７２】ログ収集要求を受信した場合は（ステップ１２０９）、正規化ログファイル４０中の正規化ログデータを補正時刻３２３の順にソートした後、ＭＡＮＡＧＥＲ＿ＡＤＤＲＥＳＳ４７１に示されるマネージャ１０へ転送する（ステップ１２１０）。

【００７３】正規化ログファイル容量確認要求を受信した場合は（ステップ１２１１）、正規化ログファイルの使用容量とＦＩＬＥ＿ＭＡＸＳＩＺＥ４７２を比較し（ステップ１２１２），最大サイズに達したとき（ステップ１２１２ＹＥＳ）は、ログ入力２０２へ中断通知を発行する（ステップ１２１３）。最大サイズに達していないとき（ステップ１２１２ＮＯ）は、前回中断要求を発行したか確認し（ステップ１２１４）、発行していたとき（ステップ１２１４ＹＥＳ）は、ログ入力２０２へログ入力再開要求を通知する（ステップ１２１５）。

【００７４】マネージャ時刻の通知を受信した場合は（ステップ１２１６）、エージェントとマネージャのコンピュータ時刻の差を計算する（ステップ１２１７）。

【００７５】終了要求を受信した場合は（ステップ１２１８）、ループを抜けて終了処理（ステップ１２１９）を行う。

【００７６】

【発明の効果】以上説明したように本発明によれば、エージェントが複数のログファイルを監視し様々の形式で出力されたログデータを入力した後，正規化を行い共通的なデータ形式に変換する。また必要なログデータだけを抽出し，ログデータの出力時刻としてマネージャの時計に合わせた補正時刻を使用するようにしたので、運用者はネットワークに存在する複数のコンピュータのログデータを統一したデータ形式及び時刻に基づいて解析することができる。

【００７７】またマネージャが蓄積するログデータについては、所定期間のログデータを保存するようにしたので、古いログデータから順に削除する形でログ情報の総量を規制できる。

【００７８】さらに収集したログデータを補正時刻及び

17

正規化項目によって検索可能としたので、運用者は必要なログ情報を容易に取得できる。

【図面の簡単な説明】

【図１】実施形態のネットワークシステムの構成図である。

【図２】実施形態のマネージャとエージェントが行う処理動作の概略を示す図である。

【図３】実施形態のマネージャ１０の構成を示す機能ブロック図である。

【図４】実施形態のエージェント２０の構成を示す機能ブロック図である。

【図５】実施形態の正規化ログデータの概略構成を示す図である。

【図６】実施形態の共通情報クラスのデータ構成を示す図である。

【図７】実施形態のユーザ情報クラスのデータ構成を示す図である。

【図８】実施形態のサービス情報クラスのデータ構成を示す図である。

【図９】実施形態のアドレス情報クラスのデータ構成を示す図である。

【図１０】実施形態のファイル情報クラスのデータ構成を示す図である。

【図１１】実施形態のトラフィフィック情報クラスのデータ構成を示す図である。

【図１２】実施形態の個別情報クラスのデータ構成を示す図である。

【図１３】実施形態のデータ格納クラスのデータ構造を示す図である。

【図１４】正規化項目のコード化テーブルの例を示す図である。

【図１５】マネージャルールの例を示す図である。

【図１６】エージェントの動作条件ルールの例を示す図である。

18

【図１７】エージェントのログファイル監視ルールの例を示す図である。

【図１８】エージェントのフォーマットルール（その１）の例を示す図である。

【図１９】エージェントのフォーマットルール（その２）の例を示す図である。

【図２０】エージェントのフィルタリングルールの例を示す図である。

【図２１】監視対象ログファイルのログデータであるメッセージテキストの例を示す図である。

【図２２】実施形態の正規化ログデータベースのデータ構造を示す図である。

【図２３】実施形態のマネージャが行うルール配布の処理の流れを示すＰＡＤ図である。

【図２４】実施形態のマネージャが行うログ収集の処理の流れを示すＰＡＤ図である。

【図２５】実施形態のマネージャが行う構成管理の処理の流れを示すＰＡＤ図である。

【図２６】実施形態のマネージャが行うデータベース管理の処理の流れを示すＰＡＤ図である。

【図２７】実施形態のエージェントが行うログ入力の処理の流れを示すＰＡＤ図である。

【図２８】実施形態のエージェントが行うログファイル管理の処理の流れを示すＰＡＤ図である。

【符号の説明】

１０・・・マネージャ、２０・・・エージェント、４０・・・正規化ログファイル、５０・・・正規化ログデータベース、６０・・・ネットワーク管理システム、１０４・・・構成管理、１０６・・・ルール配布、１０７・・・ログ収集、１０９・・・データベース管理、１１０・・・ルール、２０２・・・ログ入力、２０４・・・ログファイル管理、２０５・・・ルール

【図７】

図７

ユーザ情報クラス　～302

ユーザ名	～330
ＵＩＤ	～331
変更後のユーザ名	～332
変更後のＵＩＤ	～333
セキュリティレベル	～334
アクセス権	～335
アクセス結果	～336
端末名	～337

【図８】

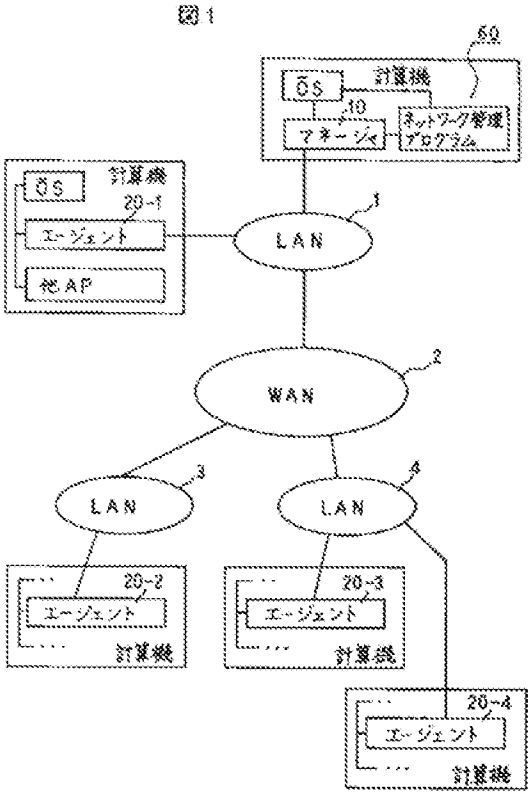
図８

サービス情報クラス　～303

サービス名	～340
サービスバージョン	～341
プロセス名	～342
プロセスＩＤ	～343

【図１】

図１



【図５】

図５

正規化ログデータ ～300

共通情報クラス	～301
ユーザ情報クラス	～302
サービス情報クラス	～303
アドレス情報クラス	～304
ファイル情報クラス	～305
・ ・ ・	
トラフィック情報クラス	～306
個別情報クラス	～307

【図６】

図６

共通情報クラス ～301

正規化バージョン		～310
ログ種別	ログ事象	～311
	ログ事象結果	～312
	ログ出力プログラム	～313
	データ格納クラス	～314
	ログファイル名	～315
マネージャ	ホスト名	～316
	ホストＩＰアドレス	～317
エージェント	ホスト名	～318
	ホストＩＰアドレス	～319
監視対象	ホスト名	～320
	ホストＩＰアドレス	～321
時刻	ログ出力時刻	～322
	補正時刻	～323
フィルタリングルール名		～324

【図１１】

図１１

トラフィック情報クラス ～306

受信バイト数
送信バイト数
処理時間

【図１２】

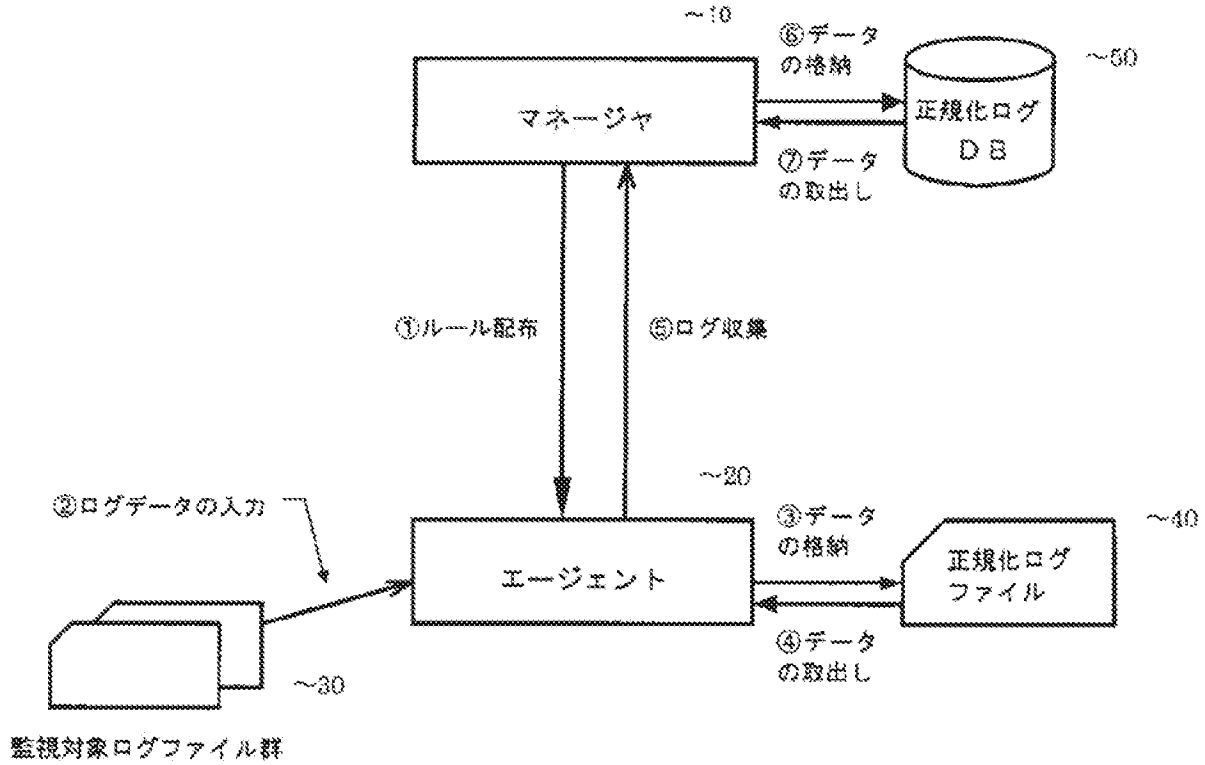
図１２

個別情報クラス ～307

メッセージテキスト

【図２】

図２



【図９】

図９

アドレス情報クラス　～304

接続元ホスト名	～350
接続元ＩＰアドレス	～351
接続元ＭＡＣアドレス	～352
接続元ポート番号	～353
接続先ホスト名	～354
接続先ＩＰアドレス	～355
接続先ＭＡＣアドレス	～356
接続先ポート番号	～357
コネクション状態	～358
開始時刻	～359
終了時刻	～360
アクセス結果	～361

【図１５】

図１５

マネージャルール　～450

LOG_MAX：ログ収集の最大多重度；　～453

【図１６】

図１６

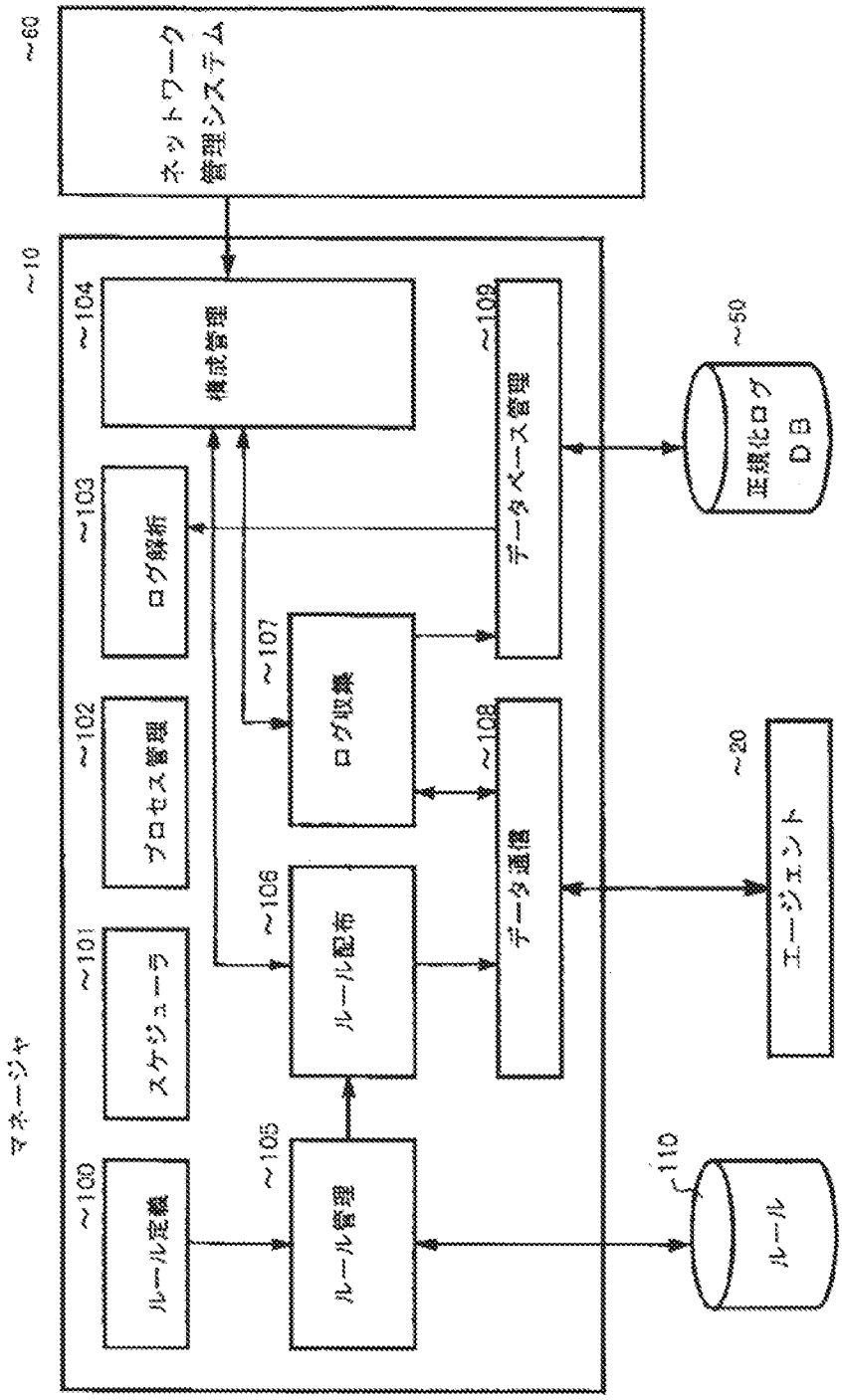
動作条件ルール　～470

MANAGER_ADDRESS：マネージャのＩＰアドレス；　～471

FILE_MAXSIZE：正規化ファイルの最大サイズ；　～472

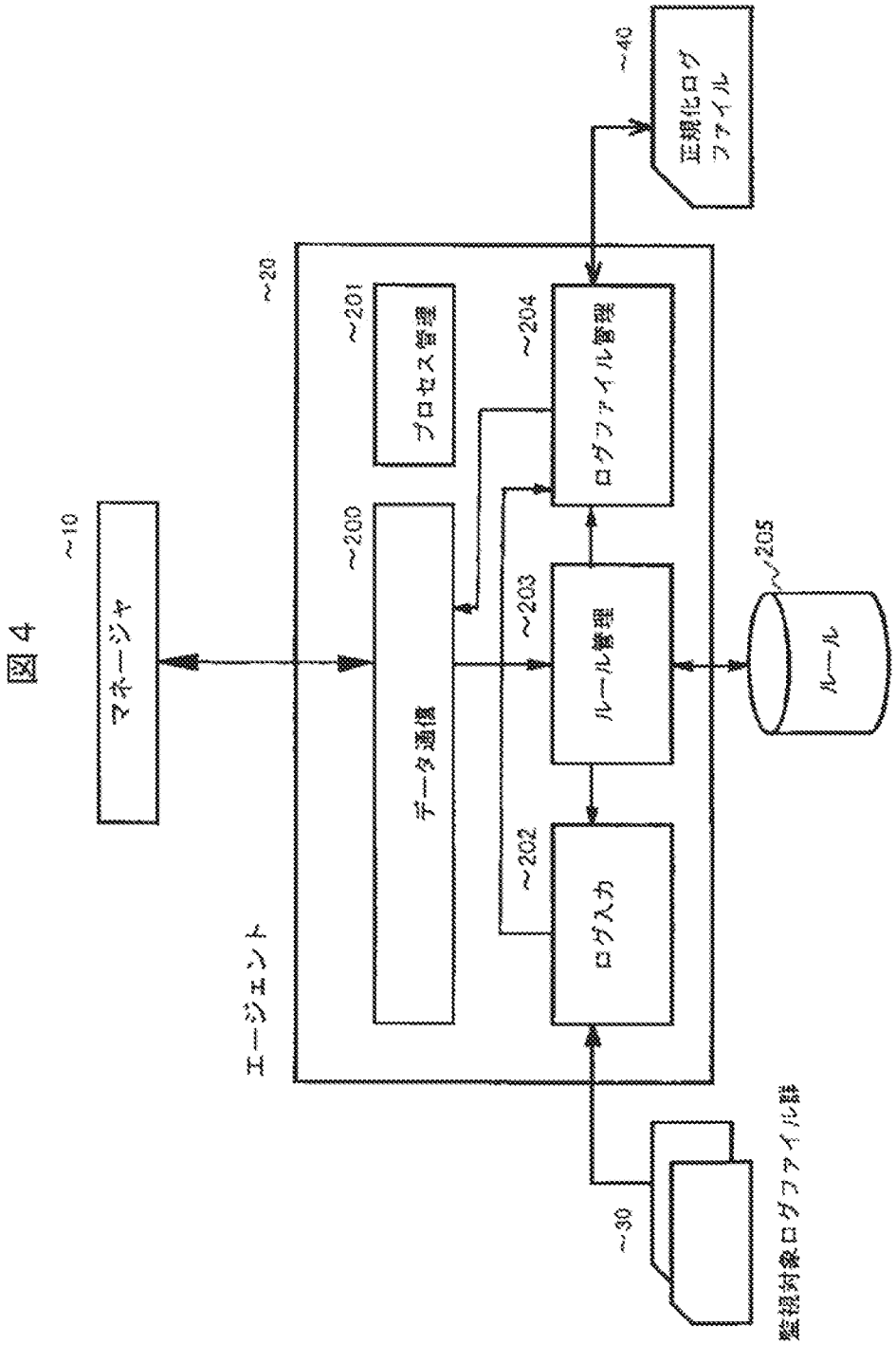
【図3】

図3


~60
ネットワーク管理システム
~10
~104
構成管理
~103
ログ解析
~102
プロセス管理
~101
スケジューラ
~100
ルール定義
~105
ルール管理
~106
ルール配布
~107
ログ収集
~108
データ通信
~109
データベース管理
~50
正規化ログDB
~20
エージェント
110
ルール
マネージャ

【図4】

図4


~10
マネージャ
~20
エージェント
~200
データ通信
~201
プロセス管理
~202
ログ入力
~203
ルール管理
~204
ログファイル管理
~205
ルール
~30
監視対象ログファイル群
~40
正規化ログファイル

【図１０】

図１０

ファイル情報クラス　～305

ファイル名	
変更後	作成時刻
	最終修正時刻
	最終アクセス時刻
	ｉ－ｎｏｄｅ番号
	アクセス許可
	ＵＩＤ
	ＧＩＤ
	サイズ
変更前	作成時刻
	最終修正時刻
	最終アクセス時刻
	ｉ－ｎｏｄｅ番号
	アクセス許可
	ＵＩＤ
	ＧＩＤ
	サイズ

【図１３】

図１３

データ格納クラス　～314

Ｔ１	Ｌ１	Ｖ１（存在する情報クラスの指定領域）						
		Ｔ２	Ｌ２	Ｖ２	Ｔ５	Ｌ５	Ｖ５	……

【図１８】

図１８

フォーマットルール（その１）　～510

```
FMT_1 : REGTEXT == "文字列１" | ログ事象 == "i" | ログ事象結果 == "0" :
正規化項目１(文字数) : 正規化項目２(終了文字) : … ;
FMT_2 : REGTEXT == "文字列２" && REGTEXT == "文字列３" | ログ事象 == "s"
| ログ事象結果 == "1" : 正規化項目１(終了文字) : SKIP(読み飛ばし文字数) :
正規化項目４(文字数) : … ;
```

【図１９】

図１９

フォーマットルール（その２）　～519

```
FMT_3 : REGTEXT == "文字列５" && REGTEXT == "文字列６" | ログ事象 == "i"
| ログ事象結果 == "1" : 正規化項目１(終了文字) : SKIP("区切り文字") : 正規
化項目２(文字数) : … ;
```

【図１７】

図１７

ログファイル監視ルール　～508

```
TARGET_LOG : "監視対象ログファイル名１", FORMAT=SEQ, INTERVAL=時間,
FMT_NAME="フォーマットルール名" ;
TARGET_LOG : "監視対象ログファイル名２", FORMAT=WRAP, INTERVAL=時間 ;
```

【図２０】

図２０

フィルタリングルール　～525

```
FLT : 正規化項目１ == "文字列１" ;
FLT : 正規化項目２ == "文字列２" || 正規化項目３ == "文字列３" ;
FLT : 正規化項目４ == "文字列４" && 正規化項目５ != "文字列５" ;
FLT : 正規化項目６ == "時刻1" - "時刻2" && 正規化項目７ == "文字列７" ;
```

【図２１】

図２１

メッセージテキスト例　～550

```
Jul 01/30 11:19 + ttyp5 fujiwa-root                                    ～551
Jul 01/31 11:32 - ttyp7 morita-sbc                                     ～552

Jan  4 12:36:10 hosta ftpd[111]: connect from 178.213.252.12           ～553
Jan 12 13:12:15 hosta ftpd[111]: refused connect from hostb            ～554
Jan 18 15:10:55 hosta ftpd[777]: connect to hostx                      ～555

Jan 25 10:12:34 hosta job[2222]: ジョブABCを開始しました。             ～556
Jan 25 10:15:19 hostx job[2222]: ジョブABCが異常終了しました。         ～557
```

【図１４】

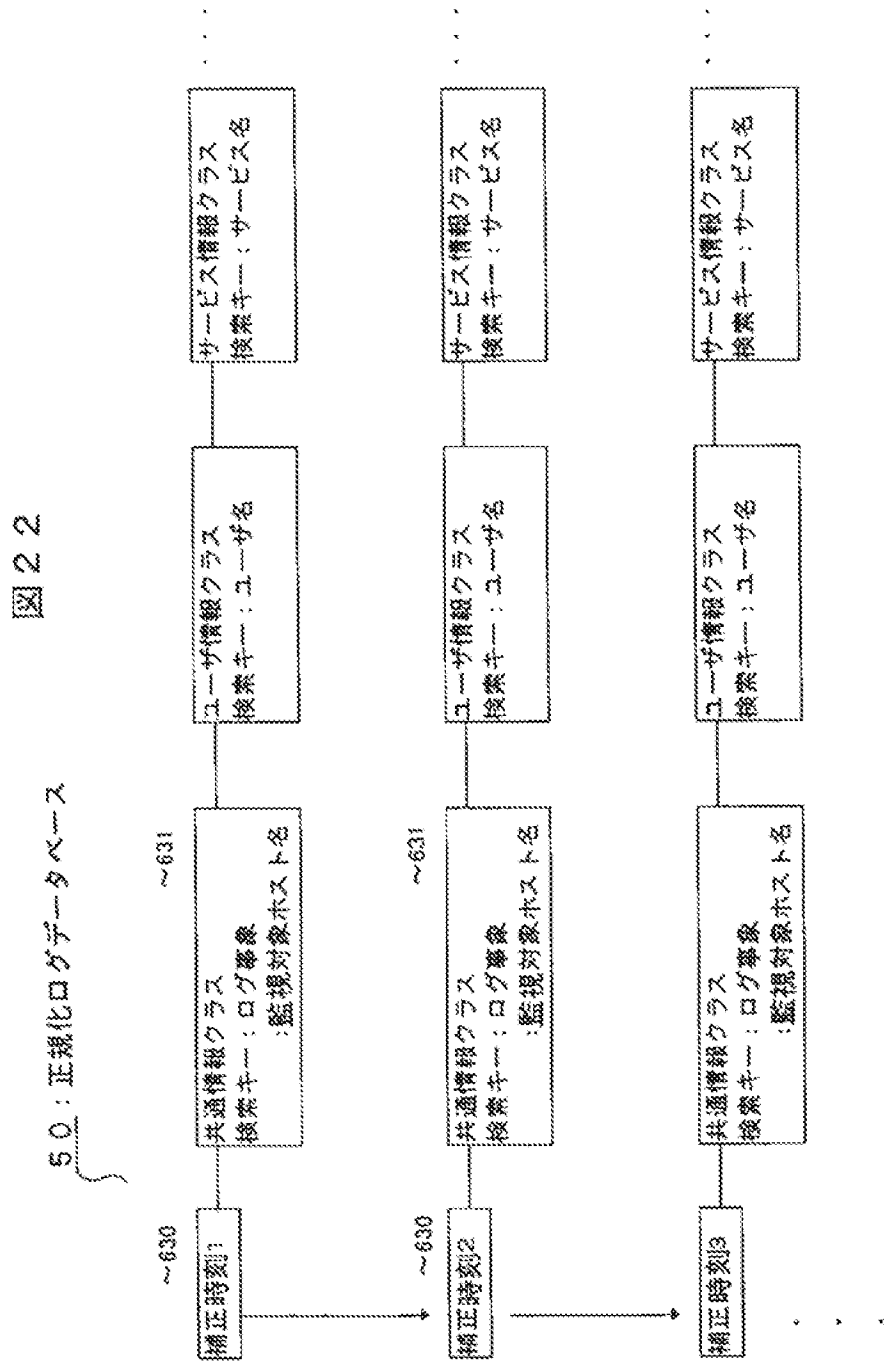
図１４

正規化項目のコード化テーブル　　～500

正規化項目	内容	コード
ログ事象	login	1
	su（ユーザ変更）	2
	connect	3
	ファイル	4
	ジョブ	5
	メール	6
ログ事象結果	成功	0
	失敗	1
アクセス権	あり	0
	なし	1
アクセス結果	成功	0
	失敗	1
アクセス許可	あり	0
	なし	1

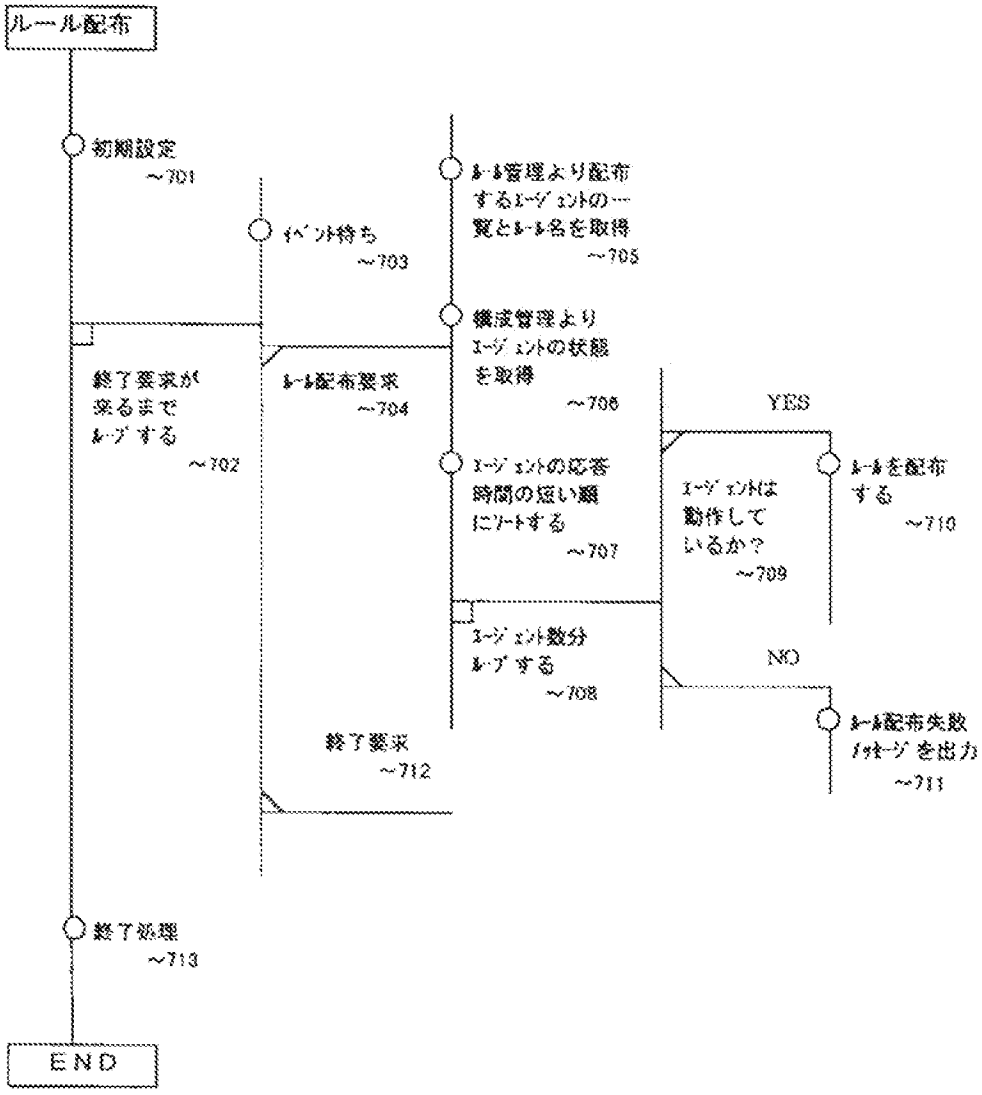
【図22】

図22


50：正規化ログデータベース
~630
~631
補正時刻1
補正時刻2
補正時刻3
共通情報クラス
検索キー：ログ事象
：監視対象ホスト名
ユーザ情報クラス
検索キー：ユーザ名
サービス情報クラス
検索キー：サービス名

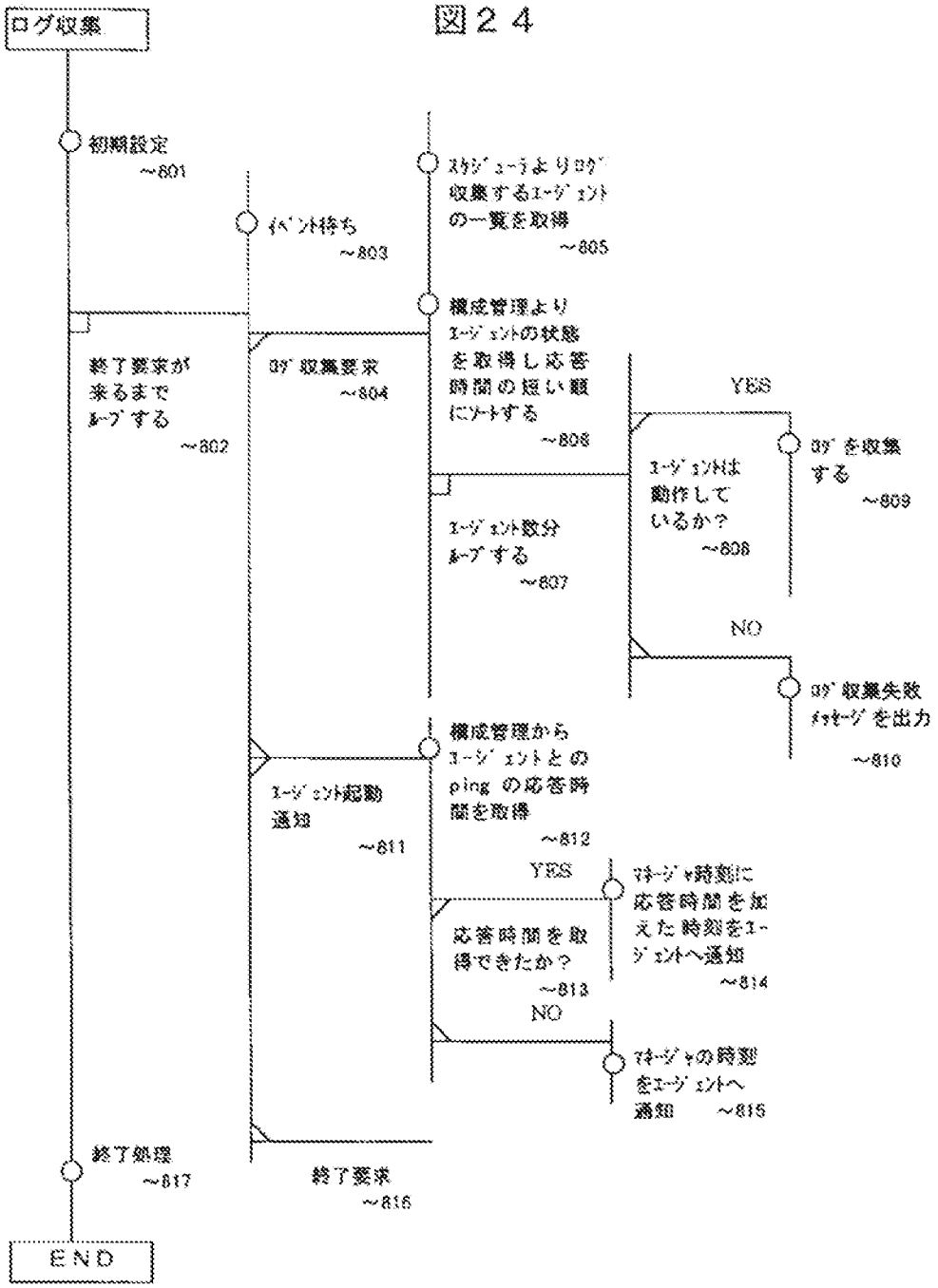
【図２３】

図２３


ルール配布
初期設定
～701
終了要求が
来るまで
ループする
～702
イベント待ち
～703
ルール配布要求
～704
ルール管理より配布
するエージェントの一
覧とルール名を取得
～705
機械管理より
エージェントの状態
を取得
～706
エージェントの応答
時間の短い順
にソートする
～707
エージェント数分
ループする
～708
YES
エージェントは
動作して
いるか？
～709
ルールを配布
する
～710
NO
ルール配布失敗
メッセージを出力
～711
終了要求
～712
終了処理
～713
END

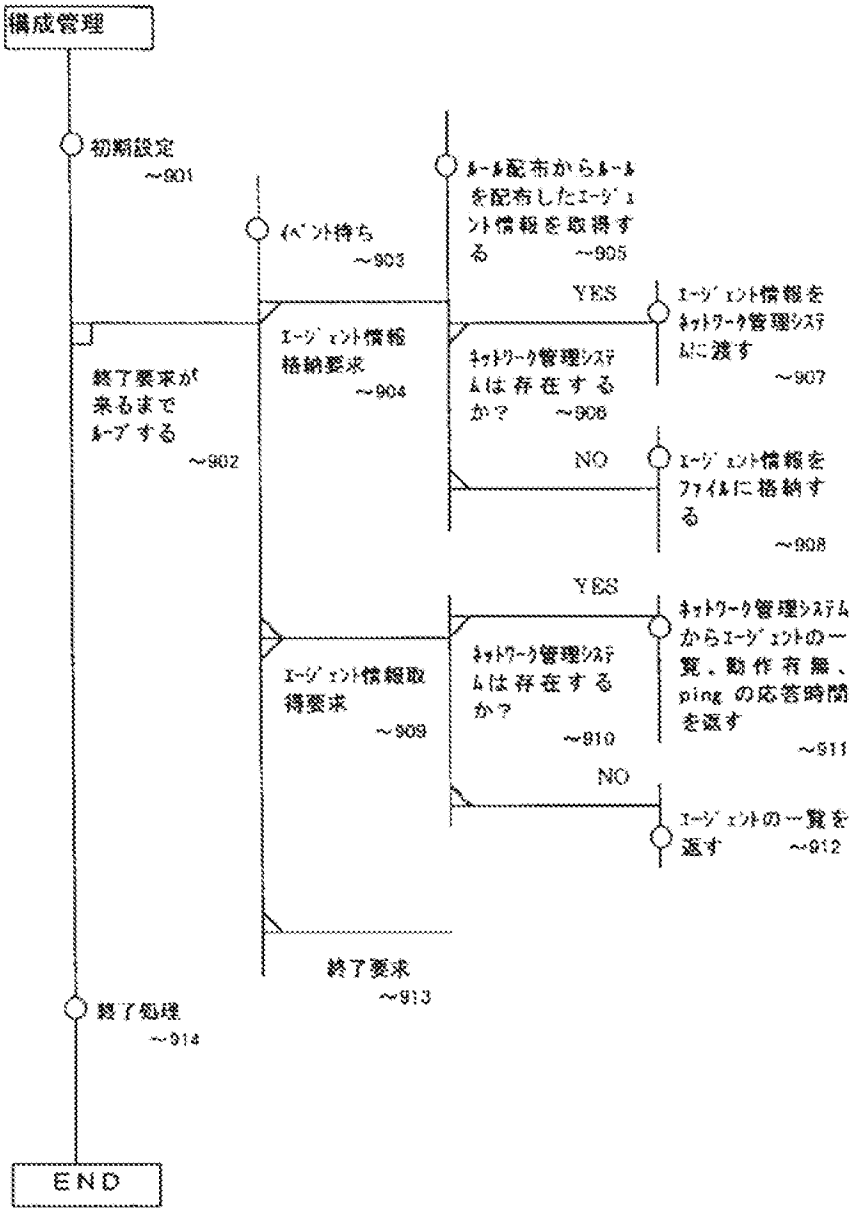
【図２４】

図２４


ログ収集
初期設定
～801
イベント待ち
～803
ｽｹｼﾞｭｰﾗよりﾛｸﾞ収集するｴｰｼﾞｪﾝﾄの一覧を取得
～805
構成管理よりｴｰｼﾞｪﾝﾄの状態を取得し応答時間の短い順にｿｰﾄする
～806
終了要求が来るまでﾙｰﾌﾟする
～802
ﾛｸﾞ収集要求
～804
YES
ｴｰｼﾞｪﾝﾄは動作しているか？
～808
ﾛｸﾞを収集する
～809
ｴｰｼﾞｪﾝﾄ数分ﾙｰﾌﾟする
～807
NO
ﾛｸﾞ収集失敗ﾒｯｾｰｼﾞを出力
～810
構成管理からｴｰｼﾞｪﾝﾄとのping の応答時間を取得
～812
ｴｰｼﾞｪﾝﾄ起動通知
～811
YES
ﾏﾈｰｼﾞｬ時刻に応答時間を加えた時刻をｴｰｼﾞｪﾝﾄへ通知
～814
応答時間を取得できたか？
～813
NO
ﾏﾈｰｼﾞｬの時刻をｴｰｼﾞｪﾝﾄへ通知
～815
終了処理
～817
終了要求
～816
END

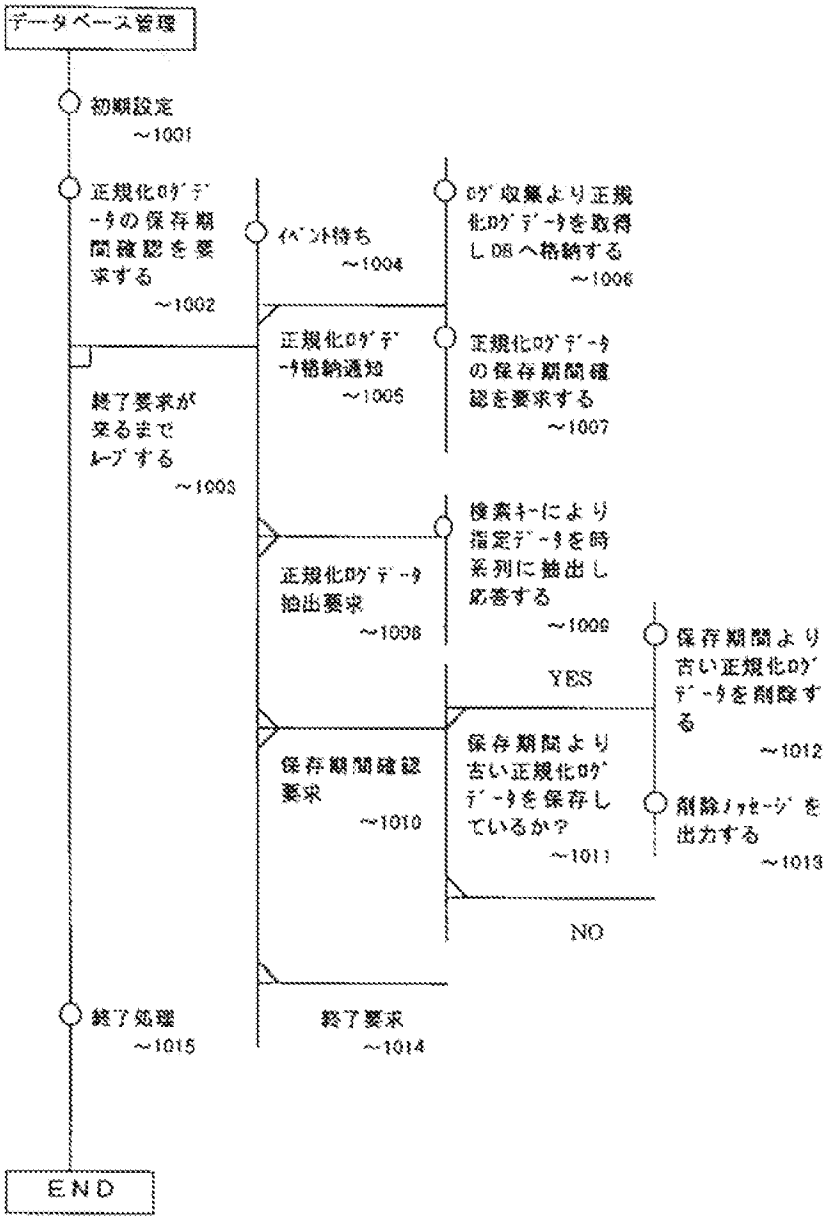
【図２５】

図２５


構成管理
初期設定
～901
イベント待ち
～903
ルール配布からルールを配布したエージェント情報を取得する
～905
YES
エージェント情報をネットワーク管理システムに渡す
～907
エージェント情報格納要求
～904
ネットワーク管理システムは存在するか？
～906
NO
エージェント情報をファイルに格納する
～908
終了要求が来るまでループする
～902
YES
ネットワーク管理システムからエージェントの一覧、動作有無、ping の応答時間を返す
～911
エージェント情報取得要求
～909
ネットワーク管理システムは存在するか？
～910
NO
エージェントの一覧を返す
～912
終了要求
～913
終了処理
～914
END

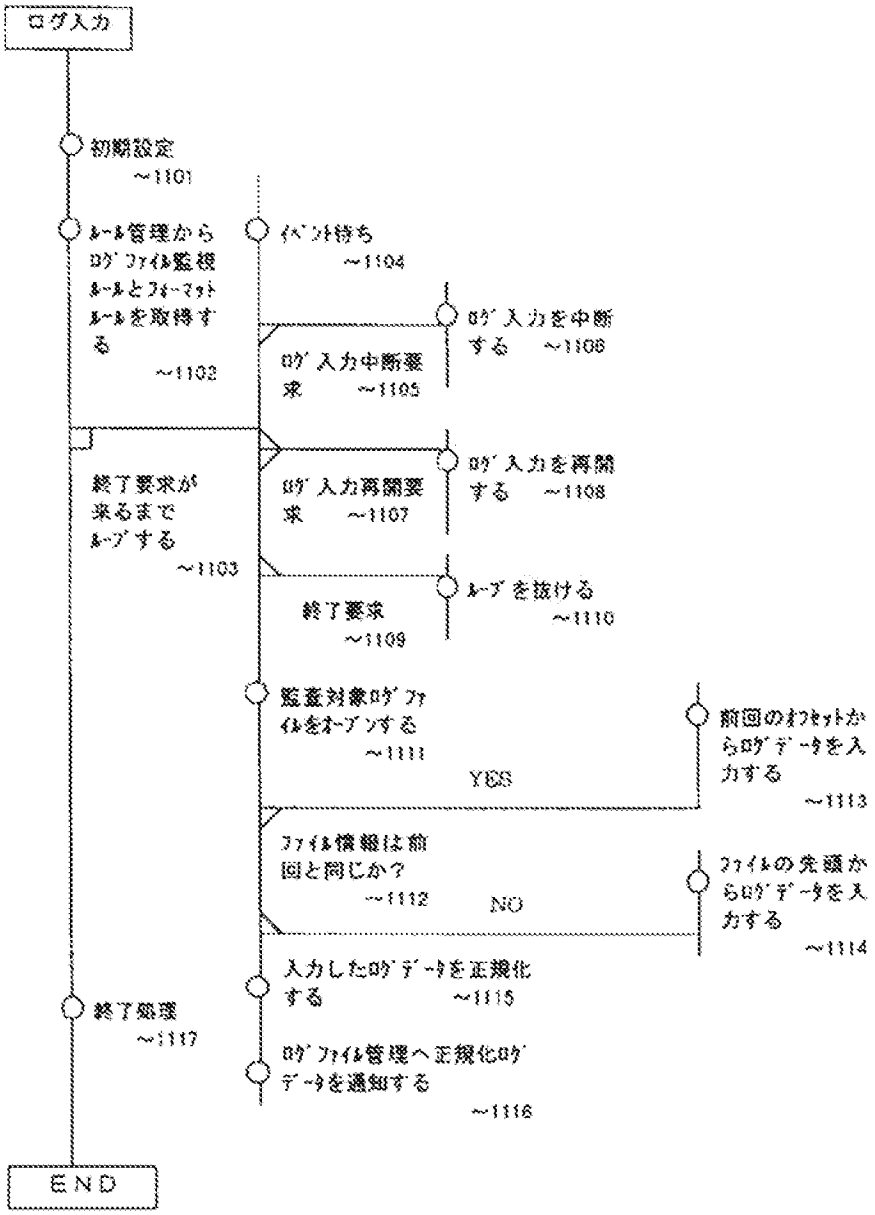
【図２６】

図２６


データベース管理
初期設定
～1001
正規化ﾛｸﾞﾃﾞｰﾀの保存期間確認を要求する
～1002
ｲﾍﾞﾝﾄ待ち
～1004
ﾛｸﾞ収集より正規化ﾛｸﾞﾃﾞｰﾀを取得しDBへ格納する
～1006
正規化ﾛｸﾞﾃﾞｰﾀ格納通知
～1005
正規化ﾛｸﾞﾃﾞｰﾀの保存期間確認を要求する
～1007
終了要求が来るまでﾙｰﾌﾟする
～1003
検索ｷｰにより指定ﾃﾞｰﾀを時系列に抽出し応答する
～1009
正規化ﾛｸﾞﾃﾞｰﾀ抽出要求
～1008
YES
保存期間より古い正規化ﾛｸﾞﾃﾞｰﾀを削除する
～1012
保存期間確認要求
～1010
保存期間より古い正規化ﾛｸﾞﾃﾞｰﾀを保存しているか？
～1011
削除ﾒｯｾｰｼﾞを出力する
～1013
NO
終了処理
～1015
終了要求
～1014
END

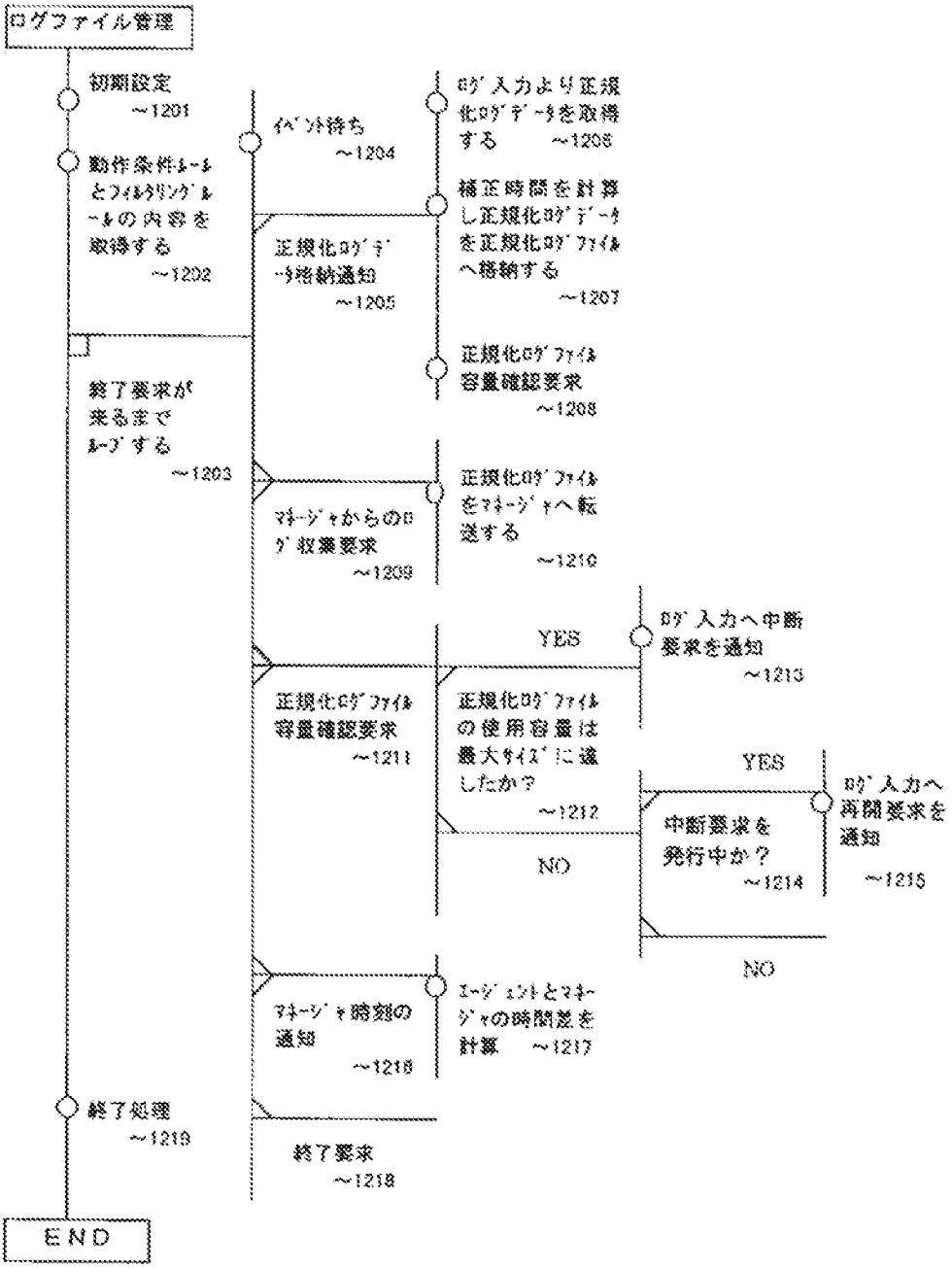
【図２７】

図２７


ログ入力
初期設定
～1101
ルール管理からログファイル監視ルールとフォーマットルールを取得する
～1102
イベント待ち
～1104
ログ入力中断要求
～1105
ログ入力を中断する
～1106
ログ入力再開要求
～1107
ログ入力を再開する
～1108
終了要求が来るまでループする
～1103
終了要求
～1109
ループを抜ける
～1110
監査対象ログファイルをオープンする
～1111
YES
前回のオフセットからログデータを入力する
～1113
ファイル情報は前回と同じか？
～1112
NO
ファイルの先頭からログデータを入力する
～1114
入力したログデータを正規化する
～1115
ログファイル管理へ正規化ログデータを通知する
～1116
終了処理
～1117
END

【図２８】

図２８



フロントページの続き

(72)発明者　中野　秀紀
東京都千代田区大手町二丁目６番２号　株式会社日立情報ネットワーク内

(72)発明者　森田　貴司
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(72)発明者　山田　貢
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(72)発明者　新村　美登
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内